FORM PTO-1449	DOCKET NO:	SERIAL NO.:	
	41230/55769	09/939,531	**RECEIVED**
INFORMATION DISCLOSURE	**APPLICANT(S):** J. Hoffstein et al.		
STATEMENT	**FILING DATE:**	**GROUP NO.:**	DEC 1 2 2001
	August 24, 2001		Technology Center 2100

UNITED STATES PATENT DOCUMENTS

EXAM. INITIALS		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES/NO
	BA						
	BB						

OTHER DOCUMENTS (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)

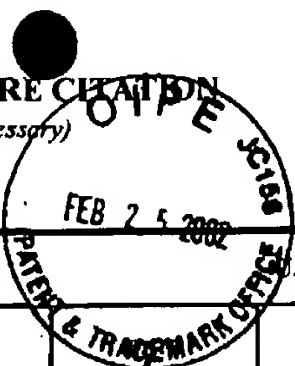|		
	CA	Con Coppersmith and Gadiel Seroussi, On the Minimum Distance of Some Quadratic Residue Codes, IEEE Transactions on Information Theory, Vol. IT-30 No. 2 March 1984, pp. 407-411,
	CB	Finite Field and Elliptic Curve Systems, Stinson Cryptography Theory and Practice, pp. 177-190
	CC	Jerome A. Solinas, Designs, Codes and Cryptography, 19, 195-249 (2000), Efficient Arithmetic on Koblitz Curves, , pp. 125-179
	CD	Chapter 14 Exponentiation, Menezen Van Oorschot and Vanstone, Handbook of Applied Cryptography, pp. 613-628
	CE	The Powering Algorithms, Henri Cohen, A Course in Computational Number Theory, pp. 8-12
	CF	Chae Hoon Lim et al., Sparse RSA Secret Keys and Their Generation, pp. 1-15. (preprint)
	CG	D.R. Stinson, Some Baby-step giant-step algorithms for the low hamming weight discrete logarithm problem, , pp. 1-15
	CH	What is a Random Sequence?, pp 149-179
	CI	Evaluation of Powers, pp. 461-481.
	CJ	Darrel Hankerson, Software Implementation of Elliptic Curve Cryptography over Binary Fields, pp. 1-24. (2000)

FORM PTO-1449		DOCKET NO: 41230/55769	SERIAL NO.: 09/939,531	RECEIVED
INFORMATION DISCLOSURE STATEMENT		APPLICANT(S): J. Hoffstein et al.		DEC 1 2 2001
		FILING DATE: August 24, 2001	GROUP NO.:	Technology Center 2100

ʄᵁᵃ	CK	Jeffrey Hoffstein, NTRU: A Ring-Based Public Key Cryptosystem, et al. pp. 268-288
ᵂ4	CL	Peter de Rooij, On the Security of the Schnorr Scheme Using Preprocessing, Eurocrypt, pp. 71-80, (1998)
ᵂ4	CM	C.P. Schnorr, Efficient Identification and Signatures for Smart Cards, pp. 239-252, (1998)
ᵂ4	CN	Jeffrey Hoffstein, NSS: An NTRU Lattice-Based Signature Scheme
ᵂᵃ	CO	Daniel M. Gordon, A Survey of Fast Exponentiation Methods, December, 1997, Journal of Algorithms 27 (1998), 129-146, pp. 1-22

EXAMINER:	Zanel	DATE: 10/11/04

GWN/rej

#5

INFORMATION DISCLOSURE CITATION
(Use several sheets if necessary)

Docket Number (Optional) 41230/55	**Application Number** 09/939,531
Applicant(s) HOFFSTEIN, et al.	
Filing Date August 24, 2001	**Group Art Unit** 2131

OIPE · JC183 · FEB 2 5 2002 · PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL	REF.	DOCUMENT NUMBER		NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
✓	AA	5,148,513	09/15/92	KOZA, et al.	395	13	
✓	AB	5,136,686	08/04/92	KOZA	395	13	
✓	AC	5,343,554	08/30/94	KOZA, et al.	395	13	
✓	AD	4,935,877	06/19/90	KOZA	364	513	

RECEIVED MAR 0 1 2002 Technology Center 2100

FOREIGN PATENT DOCUMENTS

	REF.	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	Translation YES	Translation NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

✓	CP	MENEZES, et al., Hanbook of Applied Cryptography, CRC Press, 1997, Chapter 7, 63-85.

BEST AVAILABLE COPY

EXAMINER	DATE CONSIDERED
(signature)	10/11/04

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP Section 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.